The Advanced Intelligent Network—A Security Opportunity

Thomas A. Casey, Jr.

GTE Government Systems Corporation
Communication Systems Division
77 A Street
Needham, MA 02194
617-455-4075
caseyt@mail.ndhm.gtegsc.com

Abstract

The public switched telephone network (PSTN) is evolving from a closed network made up of specialized equipment into an open network employing many of the same components and protocols that are used in the Internet. The security vulnerabilities of the Internet are well known. The possible introduction of these vulnerabilities into the PSTN provides opportunities—for hackers to exploit the vulnerabilities and for security professionals to eliminate them.

The current PSTN is evolving into what is known as the Advanced Intelligent Network (AIN). In the old PSTN, the control functions for telephone services (service logic) are implemented in software that runs in telephone switches. In the AIN, service logic is implemented by Service Logic Programs (SLPs) that run in Service Control Points (SCPs). SCPs are, in most cases, ordinary commercially available microprocessor-based workstations or servers, running the same insecure operating systems that are used on most Internet hosts. SCPs communicate with switches through the SS7 network. In addition, SCPs will have connections (sometimes via other machines) to the telephone companies' corporate data networks to support such functions as customer service and billing. There are also plans to offer customers an Internet interface for changing their service parameters—such as the number to which their calls should be forwarded.

The obvious and very interesting potential security problems created by these changes in the PSTN have received comparatively little attention from the information security community. It is the objective of this paper to change that.

1. Introduction

The public switched telephone network (PSTN) is currently undergoing some radical changes. In the past, it was a closed network made up of specialized equipment that very few people understood. Connection of customer equipment to the voice network was strictly regulated, and the control system was completely closed. Over the years, many restrictions on the connection of customer equipment to the voice network have been eliminated. Currently the same thing is happening to the control network—the SS7 network. It is evolving into an open network employing many of the same components and protocols that are used in the Internet. Connection of third-party equipment to the SS7 network is being mandated, both by federal regulations and by the marketplace. It appears that there will eventually be connections between the SS7 network and the Internet. The possible introduction of the well-known Internet security vulnerabilities into the PSTN provides opportunities—both for hackers to exploit the vulnerabilities and for security professionals to eliminate them.

In North America, Advanced Intelligent Network (AIN) is the term for the changes that the PSTN is undergoing. (In the rest of the world, these changes are known as the Intelligent Network (IN), because of differences in the evolutionary path taken by the PSTN in various parts of the world.) Section 2 of this paper is a summary of AIN concepts and terminology.

The essence of the AIN is this: In the old PSTN, the control functions for telephone services (service logic) are implemented in software that runs in telephone switches. Implementation of new services requires the (costly and risky) modification of software in thousands of switches, of a variety of models and ages. In the AIN, service logic is implemented by Service Logic Programs (SLPs) that run in Service Control Points (SCPs). New services can be implemented in one SCP (or in several, for reliability and performance reasons). One SCP can serve many switches, communicating with them via the SS7 network.

The factors contributing to the AIN security problem include the following: SCPs (and the other new components introduced by the AIN) are, in most cases, ordinary commercially available workstations or servers, running the same insecure operating systems that are used on most Internet hosts. Service logic programs are, in many cases, ordinary application programs developed by persons without any particular expertise in security. Further, the AIN objectives of rapid development and deployment of new services in response to changes in the marketplace tend to be in conflict with objectives of software correctness for reliability and security. SCPs will have connections (sometimes via other machines) to the telephone companies' corporate data networks to support such functions as customer service and billing; some of these networks are connected to the Internet. There are also plans to offer customers direct Internet interfaces for changing their service parameters—such as the number to which their calls should be forwarded. Such user interfaces could place the integrity of customers' service parameters at risk, and the Internet connections supporting them could place the integrity of the entire network at risk.

The AIN brings with it a number of interesting and challenging security problems. These problems have received relatively little attention, possibly because the inner workings of the PSTN and the AIN are unfamiliar to most members of the information security community. It is the objective of this paper to stimulate interest in these problems within the security community.

2. AIN Concepts and Terminology

This section is a very much oversimplified discussion of the AIN. It includes a high-level summary of the AIN architecture, the functions of the major components, and definitions of some of the acronyms. It is provided here in hopes of helping the reader unfamiliar with the AIN to make some sense of the terminology and the multitude of acronyms. The indulgence of readers familiar with the AIN is requested. More complete information about the AIN can be found in [Robrock91] and the extensive list of references in it.

Figure 1, on the next page, shows the major AIN components and their relationships to one another. A small subset of the total network is shown, containing at least one example of each AIN component and of the network connections between them.

In this figure, the thin solid lines represent signaling links; these links carry messages associated with the setup and teardown of individual calls. The majority of the signaling links are part of the SS7 network; the signaling links connecting the SSP to the ADJ and IP are exceptions. The thick solid lines represent voice links. Notice that the ISDN link contains both a voice and a signaling channel. The OAMP (Operation, Administration, Maintenance, and Provisioning) links carry messages associated with service deployment, with the provisioning (initial setup) of services for individual customers, and with updates to customers' service specifications. The OAMP links employ various protocols, including TCP/IP and X.25.

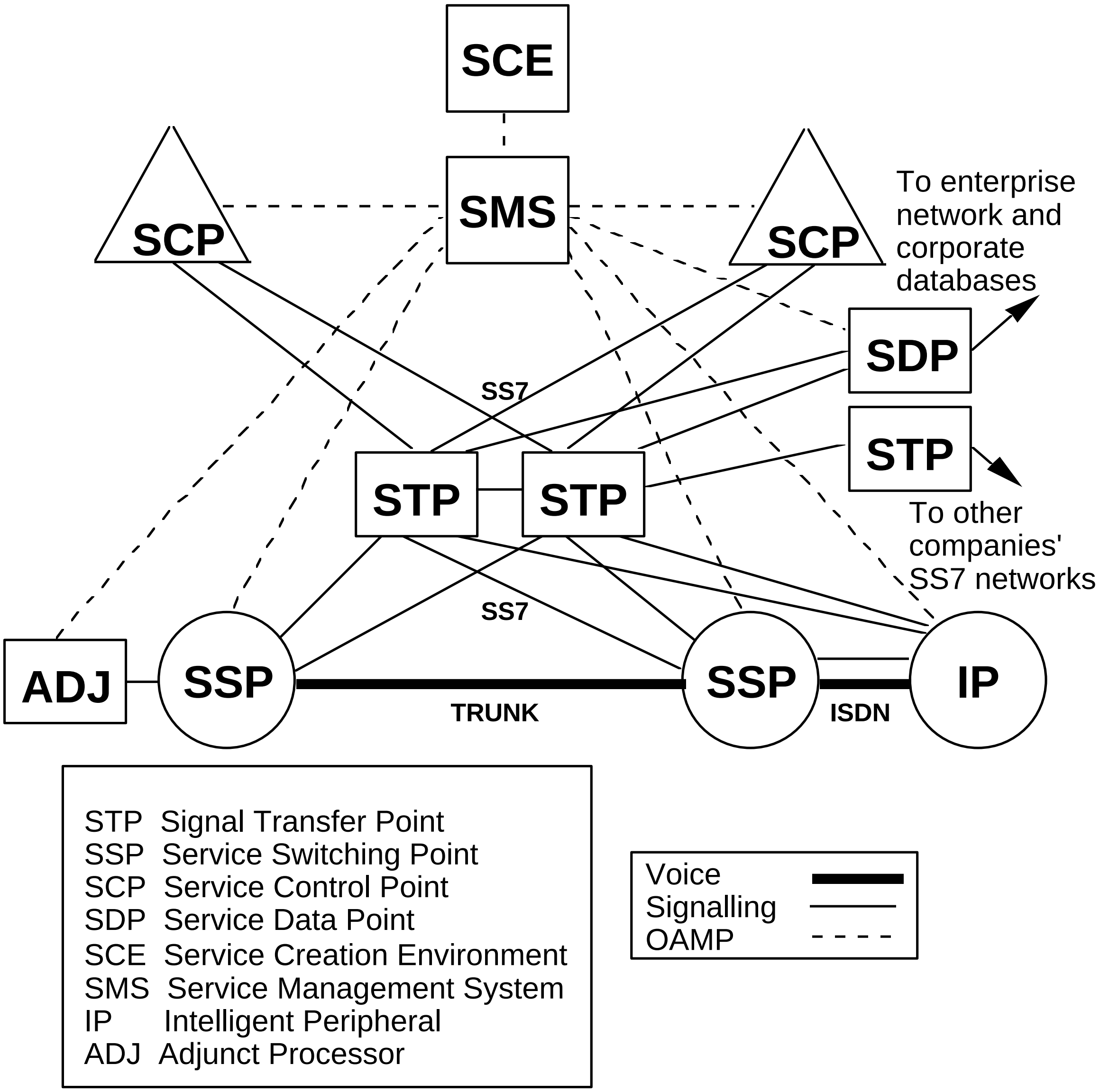
SCE
SMS
SCP
SCP
To enterprise network and corporate databases
SDP
STP
To other companies' SS7 networks
SS7
STP
STP
SS7
ADJ
SSP
SSP
IP
TRUNK
ISDN
STP Signal Transfer Point
SSP Service Switching Point
SCP Service Control Point
SDP Service Data Point
SCE Service Creation Environment
SMS Service Management System
IP Intelligent Peripheral
ADJ Adjunct Processor
Voice
Signalling
OAMP

Figure 1 - AIN Architecture

2.1 AIN Terminology

AIN has been said to stand for "Acronym-Intensive Network." Most of the AIN components have three-letter acronyms beginning with S and ending with P or F. Most of the S's stand for

"Service," most of the P's stand for "Point," and the F's stand for "Function." A point is the computer on which an architectural function is implemented, and "point code" is the term for an SS7 network address.

For each AIN component in Figure 1, Table 1 gives the acronym, the words that it stands for, and a very brief description of the component. The text that follows Table 1 briefly outlines the evolution of the AIN and describes each of the components in more detail.

SSP	Service Switching Point	Telephone switch, e.g., 5ESS, GTD-5
STP	Signal Transfer Point	SS7 packet switch
SCP	Service Control Point	The brain of the AIN; runs Service Logic Programs (SLPs)
SCE	Service Creation Environment	Development environment for SLPs
SMS	Service Management System	Deploys SLPs; provisions services for customers; updates service records
SDP	Service Data Point	Database Server for SCPs
IP	Intelligent Peripheral	Recorded messages, voice response, collection of PINs, some service logic
ADJ	Adjunct Processor	Provides SCP-like services to directly-connected switch(es) (SSPs)

Table 1 - AIN Components

2.2 Evolution of the AIN

In earlier switching systems, call setup signals were sent over the trunk lines between switches using tones similar to those emitted by touch tone phones. In Figure 1, these switches are labeled SSP (Service Switching Point).

Hackers discovered that they could build devices which they called blue boxes. These blue boxes could imitate the call setup signals and set up calls while bypassing the accounting for the calls. Thus, they were able to steal long-distance phone service.

Common Channel Signaling (CCS) eliminated this security flaw. Call setup signals are now sent between switches using a packet-switched network. The packet switches are called Signal Transfer Points (STP). The latest version of the CCS system is SS7 (Signaling System 7). At a very high level, there is some resemblance between the SS7 network and a TCP/IP network such as the Internet. However, at a more detailed level, they are quite different. The SS7 network is optimized and specialized to provide the highly reliable, real-time transfer of telephone call setup signals. More information on the SS7 network can be found in [Modaressi90].

The next step introduced a certain class of services, examples of which are nationwide 800 numbers and nationwide calling card services. These services are implemented by service logic in every switch. This logic queries either an 800 number translation database or a calling card database, in a database server known as a Service Control Point (SCP). Communication between the switch and the SCP is provided by the SS7 network. These services are, as we know, available today. (The reader might notice a discrepancy between this description and the terminology in Table 1, which gave the name Service Data Point (SDP) to the database server. The table gives the modern terminology. If we were to describe the earlier architecture using the modern terminology, we would say that the Service Data Function (SDF) was implemented in the SCP rather than in a separate SDP.)

The latest step, which the industry is now in the process of taking, moves service logic out of the switches and into the SCPs. Switches will now have trigger points in the call setup logic. At these points they can (if the appropriate trigger is enabled) send a query to an SCP asking how to proceed in the call setup. An SCP can implement one, or several, AIN services. The logic for a new service need not be added to every switch (SSP); rather, it can be implemented in one SCP (or in several for performance and availability reasons). Once the call setup logic in all switches is upgraded to include the triggers, new services can be created without requiring further modifications to switches.

2.3 AIN Components

The Service Switching Point (SSP) is a telephone switch. SSPs are present in the existing, pre-AIN PSTN. In order to participate in the AIN, a switch must be upgraded to run a version of software that conforms to the AIN call model and has triggers at specified points in the call setup sequence. If a trigger is enabled, the SSP will, at that point in call setup, send a request to the SCP asking for instructions about how to proceed with the call setup. Triggers can be enabled or disabled selectively, for individual lines, groups of lines, or the entire switch.

The Signal Transfer Point (STP) is an SS7 packet switch. These, too, are part of the existing network. There are few, if any, high level architectural changes required to the STP to support AIN services, although some detailed changes are probably required. It is likely that significant changes would be required to support enhanced security.

The Service Control Point (SCP) is the brain of the AIN. It runs Service Logic Programs (SLPs), which control call processing and provide all the new AIN services. The switch (SSP) will consult the SCP at various points in the call setup sequence. The SCP will run its Service Logic Programs, consult its (customer-specific) databases, and return instructions to the switch. There is a requirement that the instructions be returned very quickly since the switch is in the middle of a call setup and the customer is waiting for the ringing tone to start. An SCP can provide service to multiple switches. The switch and SCP communicate over the SS7 network.

The Service Data Point (SDP) is a database server for the SCPs. It implements the Service Data Function (SDF). It contains the customer-specific databases that are queried by SLPs during call setup. In earlier versions of the network, the SDF was implemented in the SCP (that is, the SCP contained its own databases). A separate database server (the SDP) is more desirable for practical reasons: there is sometimes a requirement that several SCPs be able to query a single database, and a combined SCP-SDP, along with its surrounding network., could become overloaded

The Intelligent Peripheral (IP) serves a switch (or perhaps several switches), to which it is connected by an ISDN link. It provides such services as recorded announcements, voice recognition, and the collection of DTMF tones for later transmittal, when a customer, for example, is entering a PIN number. The Adjunct Processor (ADJ) provides the adjacent SSP (to which it is connected by an Ethernet link) with SCP-like services requiring faster response than can be obtained over the SS7 network from remote SCPs. Both the ADJ and the IP can run some SLPs.

The Service Creation Environment (SCE) is a development environment for Service Logic Programs (SLPs). The Service Management System (SMS) provides an interface between the SCE and the SCP for deploying new SLPs. It also provides other management functions such as the provisioning (initial setup) of services for customers, and the updating of individual customers' call processing options.

The OAMP network is separate from the SS7 network. It connects the AIN components and carries traffic not related to the setup of telephone calls. In particular, it carries traffic related to Operation, Administration, Maintenance, and Provisioning. (Provisioning is the term used to describe the initial setup of a new service for an individual customer, as opposed to either the installation of a new service network wide, or the changing of service parameters by an individual customer on a service already provisioned.) The OAMP network uses standard protocols such as TCP/IP and X.25. It is connected to other corporate networks, and it may be connected to the Internet by gateways or dual-homed hosts.

The SSP and STP, along with the pre-AIN SCP, are part of the existing network. The new SCP, as well as the SCE, SMS, SDP, IP, and ADJ, are all being added to the network as part of the AIN. They are being implemented, for the most part, with the same standard, commercial, insecure workstations, servers, and operating systems that are found on the Internet. The AIN services are provided by ordinary application programs, written by people without any special security expertise. It is an objective of the AIN architecture to allow new telephone services to be created and deployed rapidly and inexpensively.

2.4 AIN Standards

The AIN architecture and protocols are continually being defined and refined by national and international standards groups. In North America, the work is being carried out by Standards Committee T1 - Telecommunications, Technical Subcommittee T1S1. In the international arena, the work is being done by the International Telecommunications Union (ITU), Telecommunication Standardization Sector.

Most of the work of these standards bodies has been focused on providing functionality and interoperability. In recent years, they have shown some interest in adding security to the AIN. However, while a standards body may be the appropriate forum in which to choose among several developed and tested communication protocols for worldwide standardization, it is, perhaps, a less effective forum in which to design and debug new and creative solutions to difficult security problems. In the author's opinion, it would be better for these solutions to be developed, and at least prototyped, by telephone companies and equipment vendors before being standardized.

3. The Security Problem

The magnitude of the potential security problem in the worldwide telephone network is so great that it is difficult to describe. There are potential security problems in almost all parts of the network. This paper attempts to provide a comprehensive outline of the threats and vulnerabilities, and to give a few examples. However, space limitations, as well as reluctance to describe vulnerabilities in great detail, have made it necessary to leave it to the reader's security background, expertise, and imagination to supply many of the details.

The old network was secured (to the extent that it was secured) mainly by obscurity, isolation, and physical barriers. The equipment and protocols were understood by few people, and the network interfaces were few and of limited functional capability. The AIN changes all that, by adding a great deal of new network components, protocols, connections, and interfaces.

The new components and protocols are, in many cases, identical to those that are used on the Internet; their vulnerabilities are well known. The AIN adds a great deal of new network connectivity: SS7 connections to the new components, new OAMP connections between all components (using protocols such as TCP/IP and X.25), and connections to other networks, including, in some cases, the Internet. The new customer interfaces range from the now familiar touch tone interface ("press 1 if ..."), to Internet (World Wide Web) interfaces allowing customers to change their service parameters, to direct connection of commercial customers' computers to the SS7 network. In addition to customer interfaces, there are new interfaces for telephone company employees engaged in business functions, customer care functions, and network maintenance functions. There are also new interfaces for AIN service developers (e.g., SCP writers) who may not be telephone company employees.

The new components will add vulnerabilities to the PSTN. The new connections and interfaces will make the network more accessible to those who would try to exploit those vulnerabilities. The new services, which customers will come to depend on for the conduct of their business and personal lives, will make the PSTN an even more attractive target for hackers, unscrupulous insiders, and those who would hire them in an attempt to gain some advantage for themselves or to place the telephone company or its customers at some disadvantage.

3.1 Vulnerability of Interfaces

Vulnerabilities are security weaknesses in the network. In considering vulnerabilities, we should look at all the interfaces through which an intruder might attack the telephone network. We will discuss the following interfaces:

- Customer interface
- Telco business interface
- Telco maintenance interface
- Service creation (application program) interface

- Lower layers, where there wasn't supposed to be an interface
- Law enforcement interface

The customer interface consists of the familiar touch-tone phone, plus all the other interface elements such as PBXs, pagers, cellular phones, personal computers, and in the near future, the Internet. Using this interface, customers can place calls (and by implication, agree to pay for them). They can also change their service parameters. In both cases, good security practice would require that customers be authenticated. The authentication mechanisms must be reliable, but they must also be convenient enough that customers are willing to use them. Currently popular mechanisms, such as passwords or PINs (4-digit numbers) are of dubious reliability.

Examples of abuse of the current customer interface include shoulder surfing (stealing a calling card number by watching someone make a call at a public phone), and cellular cloning (stealing the ESN (serial number) and MIN (phone number) off the air and using them in a clone phone). These abuses cost the telephone industry a great deal of money and cause customers a great deal of annoyance. The AIN adds more user interfaces and gives the users (legitimate or otherwise) of those interfaces more power to control the customer's services. For example, a call forwarding service could be abused to steal customers from a competitor (see [NYT95]).

The telco business interface is used by such people as customer service representatives, as well as people carrying out billing functions and the like. These people have access to see and modify information belonging to many customers. Because of its power, this interface should be protected by stronger authentication than that used for individual customers, to protect against the outsider threat. In addition, this interface should have its power limited by least privilege considerations, and its use should be audited, to protect against the insider threat. It is intended that the AIN will add a great deal of new and potentially complex services as quickly as the marketplace is ready for them. The number and complexity of the new services will require that customer care personnel have the ability to fix problems rapidly. If the interfaces provided to allow this were to be abused by a clever outsider or an unscrupulous insider, it could cause a great deal of trouble for both customers and the telephone companies.

The telco maintenance interface is used by people whose job it is to keep the network running. This interface includes both centralized network management systems and the direct interfaces to equipment located in, and accessible only through physical access to, switching offices. These interfaces clearly provide the ability to do significant damage to hardware or software, and they must be protected by strong authentication and strong physical security. The National Communications System AIN Program Office has studied the AIN security problem in general. Their report, now out of print, gave particular attention to the vulnerabilities of this interface.

The service creation interface adds a whole new set of vulnerabilities to the network. It is anticipated that new AIN services will be created rapidly, mostly by people who do not work for telephone companies, and who may not have a strong appreciation of the need for reliability and security in the network. A problem currently receiving much attention is the feature interaction problem, in which two services, created independently, can accidentally and innocently interfere with each other's operation. The existence of this problem points up the fact that the AIN architecture contains no provisions to prevent such interference, whether it be accidental or deliberate. The security implications of Trojan horses and trapdoors in SLPs are obvious, as are the implications of exploitable bugs introduced by accident.

The lower layer interface, where there wasn't supposed to be an interface, is included to remind the reader that one of the ways that hackers break into systems is by finding, or inventing, interfaces that were not supposed to exist. These interfaces will not be found in any design document. They exist, or the potential for them exists, only as an accidental byproduct of implementation details. (The sorts of things we have in mind here include putting a monitor on a LAN, or sending a long message that overflows a buffer and provokes the receiving program into incorrect, and possibly insecure, behavior.) At a recent telephone industry trade show, one vendor was displaying an SS7 network monitor that could passively intercept, log, and interpret all SS7 traffic.

The law enforcement interface offers a multitude of vulnerabilities. This interface is legally mandated by the Communications Assistance for Law Enforcement Act (CALEA). It requires service providers to enable the execution of lawfully authorized wiretaps and call traces. In the future this process will become more automated than in the past, allowing intercepts to be carried out by remote control. In the absence of strong security measures, the possibilities for abuse of this facility are obvious. They include: unlawful intercepts for purposes of blackmail, overzealous law enforcement, or interference with legitimate law enforcement (possibly endangering law enforcement personnel); release of lawful intercept data to unauthorized persons; suppression or alteration of intercept data to protect the guilty; and falsification of intercept data to incriminate the innocent.

3.2 Threats to the Network

Threats are actions that an intruder might take to attack the network by exploiting its vulnerabilities. The threats to the PSTN are too numerous to mention individually. This section only outlines threats and attack methods. It is best read slowly, using one's imagination.

Threats can be placed in four categories: theft of information, unauthorized alteration of information, denial of service, and theft of service. These threats can be carried out using a variety of attack methods.

The network could be attacked by three methods: physical access to network nodes or links, network access to network nodes, or the introduction of malicious software during the software development or software distribution processes. In addition, individual applications could be attacked at the end user interface by attempting to exploit weaknesses in their user authentication and usage authorization features, or by probing for flaws in their handling of incorrect input.

Attacks based on physical access to nodes could be carried out by insiders abusing their authorized access to nodes, by employees abusing their building access to gain unauthorized access to nodes, or by intruders who breach building security. Having gained access to a node, an intruder or insider could alter hardware or software, or make use of maintenance interfaces. It is possible to steal end-user or network control information, alter both types of information, or sabotage the node. Having access to, and unlimited control over, a node, an intruder could use it to launch network-based attacks on other nodes.

Network-based attacks could come from a compromised node in a telephone company's own SS7 network. Also, with the advent of mediated access, they could come from the networks of other telephone companies or third party service providers, due either to unscrupulous insiders or to lax physical security that allows intruders to gain access to nodes. In addition, an intruder having physical access to a link could attach computing equipment to it and use that equipment to carry out network-based attacks.

There are two categories of network-based attacks: passive and active. Passive attacks involve the monitoring of messages and the theft of end-user or network control information. Active attacks involve the sending of messages, often with forged sender IDs. These messages are calculated to induce the receiver to take some improper action that will result in a successful attack in one of the four threat areas (theft or alteration of information, denial of service, or theft of service). Often such messages exploit known bugs in the software in the receiving node. Defenses against both categories of network based attack involve the use of cryptography. It can provide message privacy, message authentication/integrity, or both.

Unscrupulous software developers will sometimes insert Trojan horses or trapdoors into their programs. These are pieces of malicious code that will carry out some covert function when they are installed in a production system, possibly including allowing the author to break into the system, bypassing its security features. Malicious code could also be inserted during distribution of software to the network nodes. It is an objective of the AIN architecture to allow SLPs to be written quickly and easily by a diverse set of individuals and organizations. Potentially, new SLPs could become part of the body of operating PSTN software with little or no control being exercised over their quality, correctness, or freedom from malicious code. The SLP execution environment does not impose any least-privilege constraints. Apart from implementation difficulties (involving conflicting objectives of assurance and efficiency), it is not clear how such constraints could be specified without interfering with AIN functionality. One possible solution—rigorous inspection of SLPs—is in conflict with the objective of rapid service deployment. The correct solution to this problem is not obvious.

3.3 Consequences of Attacks

Successful attacks in any of the threat areas discussed above could allow the perpetrator to accomplish one or more of a large number of consequences that are beneficial to the perpetrator but harmful to the owners and legitimate users of the network. These consequences could result in damage to individual customers—both residential and commercial—and to telephone companies. In some cases they could even threaten public safety, the national economy, or the national security. As was the case with threats, the consequences are too numerous to mention individually. They fall into the following general areas.

- Theft of private end-user information, such as voice conversations, voice mail, or data
- Theft of private telephone company information, such as customer lists, calling card numbers, or cellular authentication codes
- Alteration of end-user or telephone company information for the purpose of damaging the information resources of the victim
- Theft of, or alteration of, network control information to facilitate further penetration of the network
- Selective interference with the services of certain individuals or firms, for purposes of harassment or unscrupulous competition

- Widespread interference with network services (i.e., sabotage), or the threat of it, for purposes of terrorism or extortion
- Theft of telephone services

4. Conclusions

The problem described above is a large, multi-faceted information system security problem. It involves both computer security and network security. The problems exist in all layers, from the lowest layers of network infrastructure, up through the execution environment of application software, up to the design of the end-user interfaces.

Many of these problems could be solved by the proper application of existing computer security and network security technology. Encryption, for message privacy, message authentication, and message integrity, could provide defenses against many of the network based attacks. State of the art user authentication methods, such as smart cards for customers and telco employees, and biometric devices (e.g., fingerprint readers) controlling physical access to buildings and rooms housing switching equipment, would provide good defenses against attacks based on physical access or user interface exploitation. High assurance operating systems (those having Orange Book ratings of B2 and above) would be free of many of the exploitable vulnerabilities in the non-rated systems currently being used for AIN components. High assurance operating systems are expensive, but quantity discounts might be available if they were to be purchased in the numbers needed for the entire PSTN.

Collectively, the attendees of this conference probably have the necessary security expertise to solve the PSTN security problems. However, to secure a system it is necessary not only to understand security but also to understand the system being secured. In the author's experience, people having both security expertise and a thorough understanding of the PSTN and the AIN are rare. If these problems are to be solved, security experts and PSTN experts will have to work together and educate each other in their respective areas of expertise.

The communications network that we all depend on is undergoing changes that make it increasingly vulnerable to security problems. We, as security professionals, should work to bring these problems to the attention of the appropriate decision-makers in the telephone industry, and should take a personal interest in helping to solve them.

References

[Modaressi90] Modaressi, A.R, and R.A. Skoog, "Signaling System No. 7: A Tutorial", *IEEE Communications Magazine,* July 1990, pp. 19-34.

[NYT95] "Plumber Is Charged In Call Forwarding Theft", New York Times NATIONAL, Sunday, January 29, 1995, p. 32.

[Robrock91] Robrock, R.B., "The Intelligent Network—Changing the Face of Telecommunications", *Proceedings of the IEEE,* Vol. 79, No. 1, January 1991, pp. 7-20.